**Part I** ADMINISTRATION OF THE GOVERNMENT

**Title XV** REGULATION OF TRADE

**Chapter 93H** SECURITY BREACHES

**Section 1** DEFINITIONS

Section 1. (a) As used in this chapter, the following words shall, unless the context clearly requires otherwise, have the following meanings:—

"Agency", any agency, executive office, department, board, commission, bureau, division or authority of the commonwealth, or any of its branches, or of any political subdivision thereof.

"Breach of security", the unauthorized acquisition or unauthorized use of unencrypted data or, encrypted electronic data and the confidential process or key that is capable of compromising the security, confidentiality, or integrity of personal information, maintained by a person or agency that creates a substantial risk of identity theft or fraud against a resident of the commonwealth. A good faith but unauthorized acquisition of personal information by a person or agency, or employee or agent thereof, for the lawful purposes of such person or agency, is not a breach of security unless the personal information is used in an unauthorized manner or subject to further unauthorized disclosure.

"Data" any material upon which written, drawn, spoken, visual, or electromagnetic information or images are recorded or preserved, regardless of physical form or characteristics.

"Electronic", relating to technology having electrical, digital, magnetic, wireless, optical, electromagnetic or similar capabilities.

"Encrypted" transformation of data through the use of a 128–bit or higher algorithmic process into a form in which there is a low probability of assigning meaning without use of a confidential process or key, unless further defined by regulation of the department of consumer affairs and business regulation.

"Notice" shall include:—

(i) written notice;

(ii) electronic notice, if notice provided is consistent with the provisions regarding electronic records and signatures set forth in § 7001 (c) of Title 15 of the United States Code; and chapter 110G; or

(iii) substitute notice, if the person or agency required to provide notice demonstrates that the cost of providing written notice will exceed $250,000, or that the affected class of Massachusetts residents to be notified exceeds 500,000 residents, or that the person or agency does not have sufficient contact information to provide notice.

"Person", a natural person, corporation, association, partnership or other legal entity.

"Personal information" a resident's first name and last name or first initial and last name in combination with any 1 or more of the following data elements that relate to such resident:

(a) Social Security number;

(b) driver's license number or state-issued identification card number; or

(c) financial account number, or credit or debit card number, with or without any required security code, access code, personal identification number or password, that would permit access to a resident's financial account; provided, however, that "Personal information" shall not include information that is lawfully obtained from publicly available information, or from federal, state or local government records lawfully made available to the general public.

"Substitute notice", shall consist of all of the following:—

(i) electronic mail notice, if the person or agency has electronic mail addresses for the members of the affected class of Massachusetts residents;

(ii) clear and conspicuous posting of the notice on the home page of the person or agency if the person or agency maintains a website; and

(iii) publication in or broadcast through media or medium that provides notice throughout the commonwealth.

(b) The department of consumer affairs and business regulation may adopt regulations, from time to time, to revise the definition of "encrypted", as used in this chapter, to reflect applicable technological advancements.

**Part I** ADMINISTRATION OF THE GOVERNMENT

**Title XV** REGULATION OF TRADE

**Chapter 93H** SECURITY BREACHES

**Section 2** REGULATIONS TO SAFEGUARD PERSONAL INFORMATION OF COMMONWEALTH RESIDENTS

Section 2. (a) The department of consumer affairs and business regulation shall adopt regulations relative to any person that owns or licenses personal information about a resident of the commonwealth. Such regulations shall be designed to safeguard the personal information of residents of the commonwealth and shall be consistent with the safeguards for protection of personal information set forth in the federal regulations by which the person is regulated. The objectives of the regulations shall be to: insure the security and confidentiality of customer information in a manner fully consistent with industry standards; protect against anticipated threats or hazards to the security or integrity of such information; and protect against unauthorized access to or use of such information that may result in substantial harm or inconvenience to any consumer. The regulations shall take into account the person's size, scope and type of business, the amount of resources available to such person, the amount of stored data, and the need for security and confidentiality of both consumer and employee information.

(b) The supervisor of records, with the advice and consent of the information technology division to the extent of its jurisdiction to set information technology standards under paragraph (d) of section 4A of chapter 7, shall establish rules or regulations designed to safeguard the personal information of residents of the commonwealth that is owned or licensed. Such rules or regulations shall be applicable to: (1) executive offices and any agencies, departments, boards, commissions and instrumentalities within an executive office; and (2) any authority created by the General Court, and the rules and regulations shall take into account the size, scope and type of services provided thereby, the amount of resources available thereto, the amount of stored data, and the need for security and confidentiality of both consumer and employee information. The objectives of the rules or regulations shall be to: insure the security and confidentiality of personal information; protect against anticipated threats or hazards to the security or integrity of such information; and to protect against unauthorized access to or use of such information that could result in substantial harm or inconvenience to any resident of the commonwealth.

(c) The legislative branch, the judicial branch, the attorney general, the state secretary, the state treasurer and the state auditor shall adopt rules or regulations designed to safeguard the personal information of residents of the commonwealth for their respective departments and shall take into account the size, scope and type of services provided by their departments, the amount of resources available thereto, the amount of stored data, and the need for security and confidentiality of both consumer and employee information. The objectives of the rules or regulations shall be to: insure the security and confidentiality of customer information in a manner fully consistent with industry standards; protect

against anticipated threats or hazards to the security or integrity of such information; and protect against unauthorized access to or use of such information that could result in substantial harm or inconvenience to any resident of the commonwealth.

**Part I** ADMINISTRATION OF THE GOVERNMENT

**Title XV** REGULATION OF TRADE

**Chapter 93H** SECURITY BREACHES

**Section 3** DUTY TO REPORT KNOWN SECURITY BREACH OR UNAUTHORIZED USE OF PERSONAL INFORMATION

Section 3. (a) A person or agency that maintains or stores, but does not own or license data that includes personal information about a resident of the commonwealth, shall provide notice, as soon as practicable and without unreasonable delay, when such person or agency (1) knows or has reason to know of a breach of security or (2) when the person or agency knows or has reason to know that the personal information of such resident was acquired or used by an unauthorized person or used for an unauthorized purpose, to the owner or licensor in accordance with this chapter. In addition to providing notice as provided herein, such person or agency shall cooperate with the owner or licensor of such information. Such cooperation shall include, but not be limited to, informing the owner or licensor of the breach of security or unauthorized acquisition or use, the date or approximate date of such incident and the nature thereof, and any steps the person or agency has taken or plans to take relating to the incident, except that such cooperation shall not be deemed to require

the disclosure of confidential business information or trade secrets, or to provide notice to a resident that may have been affected by the breach of security or unauthorized acquisition or use.

(b) A person or agency that owns or licenses data that includes personal information about a resident of the commonwealth, shall provide notice, as soon as practicable and without unreasonable delay, when such person or agency (1) knows or has reason to know of a breach of security or (2) when the person or agency knows or has reason to know that the personal information of such resident was acquired or used by an unauthorized person or used for an unauthorized purpose, to the attorney general, the director of consumer affairs and business regulation and to such resident, in accordance with this chapter. The notice to be provided to the attorney general and said director, and consumer reporting agencies or state agencies if any, shall include, but not be limited to: (i) the nature of the breach of security or unauthorized acquisition or use; (ii) the number of residents of the commonwealth affected by such incident at the time of notification; (iii) the name and address of the person or agency that experienced the breach of security; (iv) name and title of the person or agency reporting the breach of security, and their relationship to the person or agency that experienced the breach of security; (v) the type of person or agency reporting the breach of security; (vi) the person responsible for the breach of security, if known; (vii) the type of personal information compromised, including, but not limited to, social security number, driver's license number, financial account number, credit or debit card number or other data; (viii) whether the person or agency maintains a written information security program; and (ix) any steps the person or agency has taken or plans to take relating to the incident, including updating the written information security program. A person who

experienced a breach of security shall file a report with the attorney general and the director of consumer affairs and business regulation certifying their credit monitoring services comply with section 3A.

Upon receipt of this notice, the director of consumer affairs and business regulation shall identify any relevant consumer reporting agency or state agency, as deemed appropriate by said director, and forward the names of the identified consumer reporting agencies and state agencies to the notifying person or agency. Such person or agency shall, as soon as practicable and without unreasonable delay, also provide notice, in accordance with this chapter, to the consumer reporting agencies and state agencies identified by the director of consumer affairs and business regulation.

The notice to be provided to the resident shall include, but shall not be limited to: (i) the resident's right to obtain a police report; (ii) how a resident may request a security freeze and the necessary information to be provided when requesting the security freeze; (iii) that there shall be no charge for a security freeze; and (iv) mitigation services to be provided pursuant to this chapter; provided, however, that said notice shall not include the nature of the breach of security or unauthorized acquisition or use, or the number of residents of the commonwealth affected by said breach of security or unauthorized access or use. The person or agency that experienced the breach of security shall provide a sample copy of the notice it sent to consumers to the attorney general and the office of consumer affairs and business regulation. A notice provided pursuant to this section shall not be delayed on grounds that the total number of residents affected is not yet ascertained. In such case, and where otherwise necessary to update or correct the information required, a

person or agency shall provide additional notice as soon as practicable and without unreasonable delay upon learning such additional information.

(c) As practicable and as not to impede active investigation by the attorney general or other law enforcement agency, the office of consumer affairs and business regulation shall: (i) make available electronic copies of the sample notice sent to consumers on its website and post such notice within 1 business day upon receipt from the person that experienced a breach of security; (ii) update the breach of security notification report on its website as soon as practically possible after the information has been verified by said office but not more than 10 business days after receipt unless the information provided is not verifiable; provided, however, that the office shall post said notice as soon as verified; (iii) amend, on a recurring basis, the breach of security notification report to include new information discovered through the investigation process or new subsequent findings from a previously reported breach of security; and (iv) instruct consumers on how they may file a public records request to obtain a copy of the notice provided to the attorney general and said director from the person who experienced a breach of security.

(d) If the person or agency that experienced a breach of security is owned by another person or corporation, the notice to the consumer shall include the name of the parent or affiliated corporation.

(e) If an agency is within the executive department, it shall provide written notification of the nature and circumstances of the breach of security or unauthorized acquisition or use to the executive office of technology services and security and the division of public records in the

office of the state secretary as soon as practicable and without unreasonable delay following the discovery of a breach of security or unauthorized acquisition or use, and shall comply with all policies and procedures adopted by the executive office of technology services and security pertaining to the reporting and investigation of such an incident.

(f) The department of consumer affairs and business regulation may promulgate regulations interpreting and applying this section.

**Part I** ADMINISTRATION OF THE GOVERNMENT

**Title XV** REGULATION OF TRADE

**Chapter 93H** SECURITY BREACHES

**Section 3A** BREACHES OF SECURITY INCLUDING SOCIAL SECURITY NUMBERS; OFFER OF CREDIT MONITORING SERVICES REQUIRED

Section 3A. (a) If a person knows or has reason to know that said person experienced an incident that requires notice pursuant to section 3 and such breach of security includes a social security number, the person shall contract with a third party to offer to each resident whose social security number was disclosed in the breach of security or is reasonably believed to have been disclosed in the breach of security, credit monitoring services at no cost to said resident for a period of not less than 18 months; provided, however, that if the person that has experienced a breach of security is a consumer reporting agency, then said consumer reporting agency shall contract with a third party to offer each resident whose social security number was disclosed in the breach of security or is reasonably believed to have been disclosed in the breach of security, credit monitoring services at no cost to such resident for a period of not less than 42 months. Said contracts shall not include reciprocal agreements for services in lieu of payment or fees. The person or agency

shall provide all information necessary for the resident to enroll in credit monitoring services and shall include information on how the resident may place a security freeze on the resident's consumer credit report.

(b) A person that experienced a breach of security shall not require a resident to waive the resident's right to a private right of action as a condition of the offer of credit monitoring services.

(c) The department of consumer affairs and business regulation may promulgate regulations interpreting and applying this section.

**Part I** ADMINISTRATION OF THE GOVERNMENT

**Title XV** REGULATION OF TRADE

**Chapter 93H** SECURITY BREACHES

**Section 4** DELAY IN NOTICE WHEN NOTICE WOULD IMPEDE CRIMINAL INVESTIGATION; COOPERATION WITH LAW ENFORCEMENT

Section 4. Notwithstanding section 3, notice may be delayed if a law enforcement agency determines that provision of such notice may impede a criminal investigation and has notified the attorney general, in writing, thereof and informs the person or agency of such determination. If notice is delayed due to such determination and as soon as the law enforcement agency determines and informs the person or agency that notification no longer poses a risk of impeding an investigation, notice shall be provided, as soon as practicable and without unreasonable delay. The person or agency shall cooperate with law enforcement in its investigation of any breach of security or unauthorized acquisition or use, which shall include the sharing of information relevant to the incident; provided however, that such disclosure shall not require the disclosure of confidential business information or trade secrets.

**Part I** ADMINISTRATION OF THE GOVERNMENT

**Title XV** REGULATION OF TRADE

**Chapter 93H** SECURITY BREACHES

**Section 5** APPLICABILITY OF OTHER STATE AND FEDERAL LAWS

Section 5. This chapter does not relieve a person or agency from the duty to comply with requirements of any applicable general or special law or federal law regarding the protection and privacy of personal information; provided however, a person who maintains procedures for responding to a breach of security pursuant to federal laws, rules, regulations, guidance, or guidelines, is deemed to be in compliance with this chapter if the person notifies affected Massachusetts residents in accordance with the maintained or required procedures when a breach occurs; provided further that the person also notifies the attorney general and the director of the office of consumer affairs and business regulation of the breach as soon as practicable and without unreasonable delay following the breach. The notice to be provided to the attorney general and the director of the office of consumer affairs and business regulation shall consist of, but not be limited to, any steps the person or agency has taken or plans to take relating to the breach pursuant to the applicable federal law, rule, regulation, guidance or guidelines; provided further that if said person or

agency does not comply with applicable federal laws, rules, regulations, guidance or guidelines, then it shall be subject to the provisions of this chapter.

**Part I** ADMINISTRATION OF THE GOVERNMENT

**Title XV** REGULATION OF TRADE

**Chapter 93H** SECURITY BREACHES

**Section 6** ENFORCEMENT OF CHAPTER

Section 6. The attorney general may bring an action pursuant to section 4 of chapter 93A against a person or otherwise to remedy violations of this chapter and for other relief that may be appropriate.

**Part I** ADMINISTRATION OF THE GOVERNMENT

**Title XV** REGULATION OF TRADE

**Chapter 93I** DISPOSITIONS AND DESTRUCTION OF RECORDS

**Section 1** DEFINITIONS

Section 1. As used in this chapter the following words shall, unless the context clearly requires otherwise, have the following meanings:—

"Agency", any county, city, town, or constitutional office or any agency thereof, including but not limited to, any department, division, bureau, board, commission or committee thereof, or any authority created by the general court to serve a public purpose, having either statewide or local jurisdiction.

"Data subject", an individual to whom personal information refers.

"Person", a natural person, corporation, association, partnership or other legal entity.

"Personal information", a resident's first name and last name or first initial and last name in combination with any 1 or more of the following data elements that relate to the resident:—

(a) Social Security number;

(b) driver's license number or Massachusetts identification card number;

(c) financial account number, or credit or debit card number, with or without any required security code, access code, personal identification number or password that would permit access to a resident's financial account; or

(d) a biometric indicator.

**Part I** ADMINISTRATION OF THE GOVERNMENT

**Title XV** REGULATION OF TRADE

**Chapter 93I** DISPOSITIONS AND DESTRUCTION OF RECORDS

**Section 2** STANDARDS FOR DISPOSAL OF RECORDS CONTAINING PERSONAL INFORMATION; DISPOSAL BY THIRD PARTY; ENFORCEMENT

Section 2. When disposing of records, each agency or person shall meet the following minimum standards for proper disposal of records containing personal information:

(a) paper documents containing personal information shall be either redacted, burned, pulverized or shredded so that personal data cannot practicably be read or reconstructed;

(b) electronic media and other non-paper media containing personal information shall be destroyed or erased so that personal information cannot practicably be read or reconstructed.

Any agency or person disposing of personal information may contract with a third party to dispose of personal information in accordance with this chapter. Any third party hired to dispose of material containing personal information shall implement and monitor compliance with

policies and procedures that prohibit unauthorized access to or acquisition of or use of personal information during the collection, transportation and disposal of personal information.

Any agency or person who violates the provisions of this chapter shall be subject to a civil fine of not more than $100 per data subject affected, provided said fine shall not exceed $50,000 for each instance of improper disposal. The attorney general may file a civil action in the superior or district court in the name of the commonwealth to recover such penalties.

**Part I** ADMINISTRATION OF THE GOVERNMENT

**Title XV** REGULATION OF TRADE

**Chapter 93I** DISPOSITIONS AND DESTRUCTION OF RECORDS

**Section 3** ENFORCEMENT

Section 3. The attorney general may bring an action pursuant to section 4 of chapter 93A against a person or otherwise to remedy violations of this chapter and for other relief that may be appropriate.

**Part I** ADMINISTRATION OF THE GOVERNMENT

**Title X** PUBLIC RECORDS

**Chapter 66A** FAIR INFORMATION PRACTICES

**Section 1** DEFINITIONS

Section 1. As used in this chapter, the following words shall have the following meanings unless the context clearly indicates otherwise:—

"Agency", any agency of the executive branch of the government, including but not limited to any constitutional or other office, executive office, department, division, bureau, board, commission or committee thereof; or any authority created by the general court to serve a public purpose, having either statewide or local jurisdiction.

"Automated personal data system", a personal data system in which personal data is stored, in whole or in part, in a computer or in electronically controlled or accessible files.

"Computer accessible", recorded on magnetic tape, magnetic film, magnetic disc, magnetic drum, punched card, or optically scannable paper or film.

"Criminal justice agency", an agency at any level of government which performs as its principal function activity relating to (a) the apprehension, prosecution, defense, adjudication, incarceration, or rehabilitation of criminal offenders; or (b) the collection, storage, dissemination, or usage of criminal offender record information.

"Data subject", an individual to whom personal data refers. This term shall not include corporations, corporate trusts, partnerships, limited partnerships, trusts or other similar entities.

"Holder", an agency which collects, uses, maintains or disseminates personal data or any person or entity which contracts or has an arrangement with an agency whereby it holds personal data as part or as a result of performing a governmental or public function or purpose. A holder which is not an agency is a holder, and subject to the provisions of this chapter, only with respect to personal data so held under contract or arrangement with an agency.

"Manual personal data system", a personal data system which is not an automated or other electronically accessible or controlled personal data system.

"Personal data", any information concerning an individual which, because of name, identifying number, mark or description can be readily associated with a particular individual; provided, however, that such information is not contained in a public record, as defined in clause Twenty-sixth of section seven of chapter four and shall not include intelligence information, evaluative information or criminal offender record information as defined in section one hundred and sixty-seven of chapter six.

"Personal data system", a system of records containing personal data, which system is organized such that the data are retrievable by use of the identity of the data subject.

**Part I** ADMINISTRATION OF THE GOVERNMENT

**Title X** PUBLIC RECORDS

**Chapter 66A** FAIR INFORMATION PRACTICES

**Section 2** HOLDERS MAINTAINING PERSONAL DATA SYSTEM; DUTIES

Section 2. Every holder maintaining personal data shall:—

(a) identify one individual immediately responsible for the personal data system who shall insure that the requirements of this chapter for preventing access to or dissemination of personal data are followed;

(b) inform each of its employees having any responsibility or function in the design, development, operation, or maintenance of the personal data system, or the use of any personal data contained therein, of each safeguard required by this chapter, of each rule and regulation promulgated pursuant to section three which pertains to the operation of the personal data system, and of the civil remedies described in section three B of chapter two hundred and fourteen available to individuals whose rights under chapter sixty-six A are allegedly violated;

(c) not allow any other agency or individual not employed by the holder to have access to personal data unless such access is authorized by statute or regulations which are consistent with the purposes of this chapter or is approved by the data subject whose personal data are sought if the data subject is entitled to access under clause (i). Medical or psychiatric data

may be made available to a physician treating a data subject upon the request of said physician, if a medical or psychiatric emergency arises which precludes the data subject's giving approval for the release of such data, but the data subject shall be given notice of such access upon termination of the emergency. A holder shall provide lists of names and addresses of applicants for professional licenses and lists of professional licensees to associations or educational organizations recognized by the appropriate professional licensing or examination board. A holder shall comply with a data subject's request to disseminate his data to a third person if practicable and upon payment, if necessary, of a reasonable fee; provided, however, that nothing in this section shall be construed to prohibit disclosure to or access by the bureau of special investigations to the records or files of the department of transitional assistance for the purposes of fraud detection and control;

(d) take reasonable precautions to protect personal data from dangers of fire, identity theft, theft, flood, natural disaster, or other physical threat;

(e) comply with the notice requirements set forth in section sixty-three of chapter thirty;

(f) in the case of data held in automated personal data systems, and to the extent feasible with data held in manual personal data systems, maintain a complete and accurate record of every access to and every use of any personal data by persons or organizations outside of or other than the holder of the data, including the identity of all such persons and organizations which have gained access to the personal data and their intended use of such data and the holder need not record any such access of its employees acting within their official duties;

(g) to the extent that such material is maintained pursuant to this section, make available to a data subject upon his request in a form comprehensible to him, a list of the uses made of his personal data, including the identity of all persons and organizations which have gained access to the data;

(h) maintain personal data with such accuracy, completeness, timeliness, pertinence and relevance as is necessary to assure fair determination of a data subject's qualifications, character, rights, opportunities, or benefits when such determinations are based upon such data;

(i) inform in writing an individual, upon his request, whether he is a data subject, and if so, make such data fully available to him or his authorized representative, upon his request, in a form comprehensible to him, unless doing so is prohibited by this clause or any other statute. A holder may withhold from a data subject for the period hereinafter set forth, information which is currently the subject of an investigation and the disclosure of which would probably so prejudice the possibility of effective law enforcement that such disclosure would not be in the public interest, but this sentence is not intended in any way to derogate from any right or power of access the data subject might have under administrative or judicial discovery procedures. Such information may be withheld for the time it takes for the holder to complete its investigation and commence an administrative or judicial proceeding on its basis, or one year from the commencement of the investigation or whichever occurs first. In making any disclosure of information to a data subject pursuant to this chapter the holder may remove personal identifiers relating to a third person, except where such third person is an officer or employee of government acting as such and the data subject is not. No holder shall

rely on any exception contained in clause Twenty-sixth of section seven of chapter four to withhold from any data subject personal data otherwise accessible to him under this chapter;

(j) establish procedures that (1) allow each data subject or his duly authorized representative to contest the accuracy, completeness, pertinence, timeliness, relevance or dissemination of his personal data or the denial of access to such data maintained in the personal data system and (2) permit personal data to be corrected or amended when the data subject or his duly authorized representative so requests and there is no disagreement concerning the change to be made or, when there is disagreement with the data subject as to whether a change should be made, assure that the data subject's claim is noted and included as part of the data subject's personal data and included in any subsequent disclosure or dissemination of the disputed data;

(k) maintain procedures to ensure that no personal data are made available in response to a demand for data made by means of compulsory legal process, unless the data subject has been notified of such demand in reasonable time that he may seek to have the process quashed;

(l) not collect or maintain more personal data than are reasonably necessary for the performance of the holder's statutory functions.

**Part I** ADMINISTRATION OF THE GOVERNMENT

**Title X** PUBLIC RECORDS

**Chapter 66A** FAIR INFORMATION PRACTICES

**Section 3** RULES AND REGULATIONS

Section 3. The secretary of each executive office shall promulgate rules and regulations to carry out the purposes of this chapter which shall be applicable to all agencies, departments, boards, commissions, authorities, and instrumentalities within each of said executive offices subject to the approval of the commissioner of administration. The department of housing and community development shall promulgate rules and regulations to carry out the purposes of this chapter which shall be applicable to local housing and redevelopment authorities of the cities and towns. Any agency not within any such executive office shall be subject to the regulations of the commissioner of administration. The attorney general, the state secretary, the state treasurer and the state auditor shall adopt applicable regulations for their respective departments.

**Commonwealth of Massachusetts**
Executive Office of Technology Services and Security (EOTSS)
Enterprise Office

# Enterprise Information Security Policy

| | |
|---|---|
| Document Name: Enterprise Information Security | Effective Date: October 15th, 2018 |
| Document ID: IS.000 | Last Revised Date: October 4th, 2018 |

Table of contents

## 1. PURPOSE

1.1. The Commonwealth of Massachusetts. ("The Commonwealth") collects, manages and stores information on a regular basis in order to support business operations. The Commonwealth is committed to preserving the confidentiality, integrity, and availability of its ***information assets****.

The Commonwealth must protect its information assets, provide for the integrity of business processes and records and comply with applicable laws and regulations.

This document, the Enterprise *Information Security Policy* (hereafter, the "Policy"), reinforces Leadership's commitment, establishes high-level functions of an information security program, and outlines information security requirements to safeguard *information assets* and assist the Commonwealth to achieve its strategic objectives.

## 2. AUTHORITY

2.1. M.G.L. Ch. 7d provides that "Notwithstanding any general or special law, rule, regulation, executive order, policy or procedure to the contrary, all executive department agencies shall, and other state agencies may, adhere to the policies, procedures and objectives established by the executive office of technology services and security with respect to activities concerning information technology."

## 3. SCOPE

3.1. This document applies to the use of information, information systems, electronic and computing devices, applications, and network resources used to conduct business on behalf of the Commonwealth. The document applies to all state agencies in the Executive Department including all executive offices, boards, commissions, agencies, departments, divisions, councils, bureaus, and offices within an executive office. Other Commonwealth entities that voluntarily use or participate in services provided by the Executive Office of Technology Services and Security, such as mass.gov, must agree to comply with this document, with respect to those services, as a condition of use.

## 4. RESPONSIBILITY

4.1. The Enterprise Security Office is responsible for the development and ongoing maintenance of this ***policy***.

4.2. The Enterprise Security Office is responsible for compliance with this policy and may enlist other departments in the maintaining and monitoring compliance with this *policy*.

4.3. Any inquiries or comments regarding this standard shall be submitted to the Enterprise Security Office by sending an email to EOTSS-DL-Security Office.

4.4. Additional information regarding this document and its related policy and standards can be found at https://www.mass.gov/cybersecurity/policies.

## 5. COMPLIANCE

5.1 Compliance with this document is mandatory. Violations are subject to disciplinary action in accordance to applicable employment and collective bargaining agreements, up to and including the termination of their employment and/or assignment with the Commonwealth.

## 6. INFORMATION SECURITY OBJECTIVES

The goal of the Information Security Program is to manage risk within the Commonwealth and achieve its information security objectives through the establishment of supporting policies, processes, and functions. The information security objectives of the Commonwealth are:

6.1 Enable organizational strategy through the protection of customer data and material non-public information.

6.2 Comply with applicable laws, regulations and contractual obligations with relevant stakeholders.

6.3 Establish a governance structure to effectively and efficiently manage information security risk.

6.4 Manage identified security risks to an acceptable (i.e., risk tolerance) level through design, implementation, and maintenance risk remediation plans.

6.5 Establish a culture of accountability and increasing the level of awareness of all personnel in order to meet information security requirements.

6.6 Establish responsibility and accountability for information security policies and governance across the Commonwealth.

The Commonwealth is committed to continually improving the Information Security Program to help ensure that its applicable information security objectives are met and it is able to adapt to changes in the cyber threat landscape and account for evolving organizational, legal and regulatory requirements.

## 7. COMMUNICATIONS

7.1. The Commonwealth's Information Security policies and standards will be publicly available on the mass.gov web site. EOTSS will inform Commonwealth agencies when policies or standards are created, or when major revisions are published.

## 8. REPORTING REQUIREMENTS

### 8.1 Policy Violations

Compliance with this document is mandatory for all state agencies in the Executive Department. Violation of this document may cause irreparable injury to the Commonwealth of Massachusetts. Violations are subject to disciplinary action in accordance with applicable employment and collective bargaining agreements, up to and including the termination of their employment and/or assignment with the Commonwealth.

### 8.2 Reporting of Policy Violations

Any violation of this policy should be reported to a supervisor and/or the Information Security Team. Information security incidents (e.g., security breaches) shall follow the reporting requirements outlined in the *Information Security Incident Management Standard.*

### 8.3 Exceptions from Policy

The policy applies to all applies to all state agencies in the Executive Department including all executive offices, boards, commissions, agencies, departments, divisions, councils, bureaus, and offices within an executive office. In the event that a policy or procedure cannot be adhered to, a policy exception request must be submitted to and approved by the Commonwealth CISO, Deputy CISO, or delegate.

An exception may be granted only if the benefits of the exception outweigh the increased risks for the approved length of the exception, as determined by the Commonwealth CISO and the associated ***Information Owner***. Compliance progress shall be validated at the exception expiration date. Exceptions may be closed if the agreed-upon solution has been implemented and the exception has been resolved. An extension may be requested if more time is required to implement the long-term solution by completing an extension request.

## 9. POLICY STATEMENTS

### 9.1 Organization of Information Security

Each organization subject to these policies shall develop, maintain and implement policies, procedures, guidelines, and standards (PSGPs) to establish and govern the Commonwealth's information security program to safeguard the confidentiality, integrity, and availability of its ***information assets***, as directed by the Commonwealth's technology leadership.

### 9.2 Acceptable Use

Personnel are the first line of defense and have a shared responsibility to safeguard information owned or entrusted to the Commonwealth.

### 9.3 Access Management

Access shall be managed throughout the account lifecycle from the initial identification of a user to the granting, modifying and revoking of user access privileges to confirm that information assets are protected from unauthorized access. Accounts shall be provisioned using the least privilege access principle. Access privileges shall be monitored and reviewed periodically commensurate with their risk

classification. Passwords must meet the Commonwealth's complexity requirements and changed on a regular basis.

### 9.4 Asset Management

Establish an information system classification schema to promote a consistent approach to risk management, business continuity and disaster recovery for information assets. Maintain an asset inventory and establish a program to manage the asset life cycle (i.e., procurement through end-of-support/end-of-life). Implement security controls to protect endpoints and mobile devices from malware and information leakage.

### 9.5 Business Continuity and Disaster Recovery

Protect mission-critical *information assets*, processes, and facilities from the effects of major failures or disasters by developing and implementing a business continuity strategy that is consistent with organizational objectives and priorities. Back up critical data, such as confidential information, and strive to prevent disasters and implement timely recovery from disasters as well as continue critical organizational functions during a disaster or major disruption while maintaining confidentiality.

### 9.6 Communication and Network Security Management

Implement network security controls such as firewalls, intrusion prevention/detection systems (IPS/IDS), virtual private networks (VPNs) and segmentation techniques so that the Commonwealth protects its *information assets* from compromise both from external and internal actors.

### 9.7 Compliance

Establish a compliance framework that will enable the Commonwealth to comply with all relevant legislative, regulatory, statutory and contractual requirements related to information security.

### 9.8 Cryptographic Management

Define requirements for encrypting data at rest, data in transit and data in use, commensurate with the information classification of the information requiring protection. Maintain cryptographic keys to preserve the integrity of cryptographic controls. Use of encryption controls shall be determined after a risk assessment has been performed.

### 9.9 Information Security Incident Management

Establish a program to effectively detect, respond and resolve incidents that affect the security of the Commonwealth's ***information assets***, including establishing a Security Incident Response Team (SIRT) to manage the incident response process. Develop incident response procedures/plans and identify relevant stakeholders (both internal and external). Test incident response plans periodically for relevancy.

### 9.10 Information Security Risk Management

Identify and analyze information security risks that could compromise the confidentiality, integrity or availability of the Commonwealth's ***information assets***, and mitigate them to an acceptable level to meet organizational objectives and compliance requirements. All relevant statutory, regulatory and contractual requirements that include security and privacy controls and the Commonwealth's approach to meet these requirements must be explicitly defined, documented and kept up to date.

### 9.11 Logging and Event Monitoring

Develop and implement a process to monitor and review activity on information systems. So that information system problems are identified and corrected, and operator logs and fault logging are

enabled, collected and reviewed. The Commonwealth must comply with all relevant legal, regulatory and contractual requirements applicable to logging and event monitoring.

9.12 Operations Management

Develop and document standard operating procedures, change management, configuration management, capacity management and release management processes for technology environments. Back up information in a secure manner to enable the organization to restore its operational activities after a planned or unplanned interruption of service.

Establish standards to support the secure implementation of applications and services in public and private cloud environments, including Software as a Service (SaaS), Platform as a Service (PaaS) and Infrastructure as a Service (IaaS).

9.13 Physical and Environment Security

Enforce physical security controls to manage access to ***information assets***. Physically protect facilities with safeguards to protect ***information assets*** against environmental hazards.

9.14 Secure System and Software Life Cycle Management

Perform information security reviews throughout all phases of the system and software management lifecycle to ensure risks are properly identified, addressed and mitigated in a timely and cost-efficient manner. Configure systems using security hardening standards and review configurations periodically.

9.15 Third-party Information Security

Establish a process to perform initial and ongoing due diligence of third parties that enter into formal business arrangements with Commonwealth agencies. Contractual agreements between third parties and Commonwealth agencies must address baseline information security clauses, including, but not limited to, the right to audit and adhere to data protection requirements.

9.16 Vulnerability Management

Implement security controls to manage and monitor risks to the Commonwealth's information technology environment. Vulnerability management personnel must be able to identify and respond to vulnerabilities within established and predictable timeframes. Vulnerability management activities must be reported to management periodically.

## 10. POLICY FRAMEWORK COVERAGE

| Policy ref. | Policy/Standard name | Topics covered |
|---|---|---|
| IS 001 | Organization of Information Security | • Information Security Organization Structure<br>• Roles and Responsibilities<br>• Policy Framework<br>• Policy Life Cycle Management |
| IS 002 | Acceptable Use of Information Technology | |
| IS 003 | Access Management | • User and System Access Management<br>• Account Management<br>• Password Management |

| Policy ref. | Policy/Standard name | Topics covered |
|---|---|---|
| IS 004 | Asset Management | • Information Asset Management<br>• Information Protection Requirements<br>• Information Classification<br>• Information System Classification<br>• Information Labeling and Handling<br>• Endpoint Security<br>• Information Disposal<br>• Mobile Device Management |
| IS 005 | Business Continuity and Disaster Recovery | • Business Continuity<br>• Disaster Recovery |
| IS 006 | Communication and Network Security | • Network Security Management<br>• Remote Access Security Management<br>• Secure File Transfer<br>• Management of Third-party Network Access |
| IS 007 | Compliance | • Compliance with Policies, Standards, Guidelines, and Procedures<br>• Reporting Security Incidents and Violations<br>• Security Compliance Reviews<br>• External Attestation of Compliance |
| IS 008 | Cryptographic Management | • Key Management<br>• Approved Cryptography Techniques |
| IS 009 | Information Security Incident Management | • Information Security Incident Management |
| IS 010 | Information Security Risk Management | • Information Security Risk Management<br>• Security Awareness and Training |
| IS 011 | Logging and Event Monitoring | • Logging and Event Monitoring |
| IS 012 | Operations Management | • Standard Operating Procedures<br>• Change Management<br>• Configuration Management<br>• Capacity Management<br>• Release Management<br>• Data Backup and Restoration<br>• Cloud Computing |
| IS 013 | Physical and Environment Security | • Facility Controls and Secure Areas<br>• Equipment and Other Media Security |
| IS 014 | Secure System and Software Lifecycle Management | • Security in System and Software Life Cycle<br>• Security in SDLC Support Processes<br>• System Hardening |
| IS 015 | Third Party Information Security | • Contractual Security Risk Identification<br>• Third-party Selection<br>• Contractual Security Provisions<br>• Third-party Life Cycle Management |
| IS 016 | Vulnerability Management | • Vulnerability and Patch Management |
| N/A | Glossary of Terms | N/A |

Table 1 — Policy Structure

## 11. DOCUMENT CHANGE CONTROL

| Version No. | Revised by | Effective date | Description of changes |
|---|---|---|---|
| 0.80 | Jim Cusson | 10/01/2017 | Corrections and formatting. |
| 0.90 | John Merto | 12/18/2017 | Minor corrections, wording. |
| 0.95 | Sean Vinck | 5.7.18 | Minor corrections and formatting. |
| 0.96 | Andrew Rudder | 5/31/2018 | Corrections and formatting |
| 0.97 | Anthony O'Neill | 05/31/2018 | Corrections and formatting |
| 1.0 | Dennis McDermitt | 06/01/2018 | Final pre-publication Review |
| 1.0 | Andrew Rudder | 10/4/2018 | Approved for Publication by: John Merto |

The owner of this document is the Commonwealth CISO (or designee). It is the responsibility of the document owner to maintain, update and communicate the content of this document. Questions or suggestions for improvement must be submitted to the document owner.

*11.1 Annual Review*

This *Enterprise Information Security Policy* must be reviewed and updated by the document owner on an annual basis or when significant policy or procedure changes necessitate an amendment.